UNITED STATES DISTRICT COURT
EASTERN DISTRICT OF MISSOURI
EASTERN DISTRICT

UNITED STATES OF AMERICA,	)	
	)	
Plaintiff,	)	
	)	
v.	)	No. 4:16 CR00374 JAR (PLC)
	)	
ROLAND HOEFFFENER,	)	
	)	
Defendant.	)	

GOVERNMENT'S RESPONSE TO DEFENDANT'S MOTION TO SUPPRESS EVIDENCE, STATEMENTS, AND *FRANKS* HEARING REQUEST

Comes now the United States of America, by and through its attorneys, Carrie Costantin, Acting United States Attorney for the Eastern District of Missouri, and Colleen Lang, Assistant United States Attorney for said district, and files its Response to Defendant's Motions to Suppress Evidence and Statements and Motion for a *Franks* hearing.

I. INTRODUCTION

Defendant moves to suppress evidence seized from defendant's residence pursuant to a state search warrant on the grounds that the information in the affidavit was obtained from an illegal online search by an undercover officer. Additionally, defendant has moved to suppress his statements made to law enforcement officers at his residence and at the police station. Specifically, defendant argues that the statements made at his residence were obtained without the defendant being properly advised of his Fifth and Sixth Amendment Rights. Defendant lastly requests a *Franks* hearing. The Government responds to all three motions in this one brief.

The evidence presented within this response and at the hearing will show that the affidavit in support of the search warrant was supported by probable cause and did not rely on illegally obtained evidence. Defendant did not have a reasonable expectation of privacy in files that he shared with a law enforcement officer and law enforcement did not conduct an illegal search. Further, the descriptions in the affidavit were sufficient to satisfy the required probable cause standard. In addition, the testimony will demonstrate that the statements the defendant made to law enforcement officials at his residence were voluntary, non-custodial statements. Also, the testimony will establish that the statements made at the police station were given in response to proper *Miranda* warnings, that the defendant understood those warnings, and that the statements were voluntary. Finally, the defendant has not made a substantiated preliminary showing to warrant a *Franks* hearing.

II. FACTUAL BACKGROUND[1]

A. BitTorrent Network/Torrential Downpour

BitTorrent is a free, publicly available, peer-to-peer file sharing program on the internet that allows different computer users to trade videos, images, and music files from one computer to another. A BitTorrent user's computer can simultaneously provide files to other BitTorrent users while downloading files from other users on the network. The BitTorrent network can be accessed via many different BitTorrent network programs, such as uTorrent.

During the installation of typical BitTorrent network client programs, various settings are established which configure the host computer to share files via automatic uploading. Typically, as users download files or pieces of files from other peers/clients on the BitTorrent network,

1 The background and factual summary information provided is intended as a general guide to aid the Court. It is not intended as a comprehensive statement of the government's case.

other peers/clients on the network are able to download the files or pieces of files from them, a process, which maximizes the download speeds for all users on the network.

Files or sets of files are shared on the BitTorrent network via the use of “Torrents” (also “.torrents”). A Torrent is typically a small file that describes the file(s) to be shared. It is important to note that Torrent files do not contain the actual file(s) to be shared, but information about the file(s) to be shared. This information includes the “info hash,” which is a SHA-1 hash value of the set of data describing the file(s) referenced in the Torrent. This set of data contains the SHA-1 hash value of each file piece in the Torrent, the file size(s), and the file name(s). This “info hash” uniquely identifies the Torrent file on the BitTorrent network. See Exhibit 1, Affidavit in Support of Search, ¶ 19; Exhibit 2, Robert Erdely’s Affidavit ¶ 6.

In order to locate Torrent files of interest and download the files that they describe, a typical user will use keyword searches on Torrent-indexing websites, examples of which include isohhunt.com and the piratebay.org. Torrent-indexing websites do not actually host the content (files) described by Torrent files, only the Torrent files themselves. Once a Torrent file is located on the website that meets a user’s keyword search criteria, the user will download the Torrent file to their computer. The BitTorrent network client program on the user’s computer will then process that Torrent file to help facilitate finding other peers/clients on the network that have all or part of the file(s) referenced in the Torrent file.

Typically, once the BitTorrent network client has downloaded part of a file(s), it may immediately begin sharing the file(s) with other users on the network. The downloaded file(s) are then stored in an area or folder previously designated by the user on the user’s computer or on an external storage media. The downloaded file(s), including the Torrent file, will remain in that location until moved or deleted by the user. Ex. 2, ¶ 8; ¶ 15.

Law enforcement can search the BitTorrent network in order to locate individuals sharing child pornography images, which have been previously identified as such based on their SHA1 values. Law enforcement uses BitTorrent network client programs which allow for single-source downloads from a computer at a single IP address, meaning that an entire file(s) is downloaded only from a computer at a single IP address as opposed to obtaining the file from multiple peers/clients on the BitTorrent network. This procedure allows for the detection and investigation of those computers involved in sharing digital files of known or suspected child pornography on the BitTorrent network. *Id.* at ¶ 12.

A peer-to-peer file transfer is assisted by reference to an Internet Protocol ("IP") address. This address, expressed as four numbers separated by decimal points, is unique to a particular computer device during an online session. The IP address provides a unique location, making it possible for data to be transferred between computers. Ex. 1, Affidavit ¶ 13.

The computer running the file sharing application, in this case a BitTorrent application, has an IP address assigned to it while it is on the internet. BitTorrent users are able to see the IP address of any computer system sharing files to them or receiving files from them. Investigators log the IP address, which has sent those files or information regarding files being shared. Investigators can then search public records that are available on the internet to determine the internet service provider who has assigned that IP address. Based upon the IP address assigned to the computer sharing files, subscriber information can be obtained from the internet service provider via subpoena.

Accordingly, in order to effectively use a peer-to-peer client software using the

BitTorrent protocol, a user is making several pieces of information publically available to all other users of the peer-to-peer network: (1) the IP address of his/her computer, which is necessary to share files between computers on the network (like a delivery address); (2) that the user's computer is employing a particular peer-to-peer client program (here, a BitTorrent program); and (3) the content of any files a user is sharing via that peer-to-peer program, which the user – either by default, or by selection – has made available for other users to download through the peer-to-peer network.

"Roundup Torrential Downpour" also known as "Torrential Downpour" is software used by law enforcement to identify potential possessors and distributors of child pornography over the BitTorrent network. Law enforcement on the BitTorrent network are identifying potential sharers of child pornography in essentially the same way that any other individual peer-to-peer user seeking to share child pornography identifies a potential source of that child pornography. Ex. 2, ¶ 3; ¶ 4. Torrential Downpour adheres to the BitTorrent protocol and connects in the same manner as any other BitTorrent client. Torrential Downpour does not have access to data or content that is not available to non-law enforcement BitTorrent applications.

There are a few very minor differences between the ICAC law enforcement system's use of the BitTorrent peer-to-peer system and a "peer's" use of the peer-to-peer system. 1) Ordinary BitTorrent users must obtain a .torrent file before they can seek a given file from another peer through a BitTorrent network. The ICAC law enforcement system, however, maintains those .torrent files and hash values, so the ICAC investigators do not have to search outside websites for that information. 2) Law enforcement uses software to engage in a single-source download from a solitary download candidate. This is an example of Law Enforcement being more restrictive than the original design of BitTorrent, which seeks to download from many sharing computers to speed up the download times. Furthermore, single source downloads do not affect what data or content is made available on the network. 3) Law enforcement software does not share any of the content downloaded during an investigation. Ex. 2, ¶11-13.

Torrential Downpour software works very similar to an ordinary client on BitTorrent and based upon how the BitTorrent download process works, it would be absolutely impossible to randomly download files from a suspect's computer which are from "unshared folders." Without a torrent file (the instructions), two BitTorrent programs would not be able to share any files. Ex. 2, ¶ 16.

Factual Background

i. Det. Baine's Investigation

While using BitTorrent software designed for law enforcement called RoundUp Torrential Downpour (hereinafter "Torrential Downpour") on the BitTorrent network, on or about December 15, 2012, Det. Bobby Baine with St. Louis Metropolitan Police Department located an IP address of 76.215.116.247 possessing or offering to share files of child pornography. Det. Baine was able to download child pornography images and child erotica images from that IP address. During the connection, the defendant's computer acknowledged having all of the files, 1128 of 1128 pieces of the file. The connection with the defendant's computer, besides being a single source download, was consistent to how all connections are made on the BitTorrent network.

In addition to the actual images of child pornography, the Torrential Downpour program captured various data – all of which was made publically available by the host computer through its use of the peer-to-peer client software. This data included the computer's IP address and the peer-to-peer client software being utilized by the host computer to share files via the

BitTorrent protocol. Log files recording the details of these downloads were also automatically created by Torrential Downpour to memorialize the downloads.

Account information received from AT&T internet services stated that the subscriber of that IP address was Roland Hoeffener at 625 Mildred Avenue, Webster Groves, Missouri. This address is located in the Eastern District of Missouri. An Ameren UE utilities inquiry showed a Mary Beth Hoeffener residing at the home. This information was sent to the St. Louis County Police Department.

ii. Search Warrant Execution

On April 29, 2013, Det. Dustin Partney of the St. Louis County Police Department drafted a state search warrant for the defendant's home based upon the information he received from Det. Baine, as well as information he collected on the case. That same day, the search warrant was signed by St. Louis County Judge Bresnahan. Ex. 1. The search warrant affidavit listed and described in detail two particular images of child pornography downloaded from the subject IP address. These images are child pornography in accordance with the *Dost* factors. See *United States v. Dost*, 636 F.Supp. 828 (S.D.Cal.1986). Ex. 1.

On April 30, 2013, the search warrant was executed upon the defendant's home by members of the St. Louis County Police Department. No one was home at the time the search warrant was executed. In accordance with standard procedure, the St. Louis County Police Department's Tactical Operation Team made entry into the home first. After the home was cleared, the Tactical Operations Team left the scene, and Sgt. Adam Kavanaugh called Mary Beth Hoeffener. Sgt. Kavanaugh informed Ms. Hoeffener of the investigation and asked that her and her husband respond home. About twenty (20) minutes later, Ms. Hoeffener, and her husband, Roland Hoeffener, responded home. Det. Partney explained to Ms. Hoeffener the reason for the warrant and she stated that she was unaware of any illegal activity coming from her home.

Sgt. Kavanaugh then talked to Roland Hoeffener, the defendant, and advised him of the investigation. At this point the Tactical Operations Team had left the scene. Most police officers at the scene were wearing street clothes. Det. Davis and Det. Roediger searched the home for computers and seized computer evidence.

iii. Defendant's Statements

The defendant voluntarily agreed to speak with Sgt. Kavanaugh in his unmarked police car. The conversation began casual and the defendant voluntarily consented to speak with Sgt. Kavanaugh. The conversation was without any coercion, non-custodial, and remained non-confrontation throughout[2]. The defendant was not under arrest. It was recorded by audio tape. The defendant was not handcuffed or restrained. The defendant told Sgt. Kavanaugh that he owned about seven computers and had lived in his home for twenty-five years. The defendant stated he had secure Wi-Fi internet service through AT&T and had used uTorrent, a peer-to-peer network, to download music and adult pornography. Sgt. Kavanaugh told the defendant based on their investigation, they knew that someone at the home had downloaded files that contained child pornography. Defendant admitted that some of his downloads did contain child pornography. Defendant stated he would occasionally search for child pornography using terms such as, "PTHC" and "teen." Defendant told Sgt. Kavanaugh that the child pornography would be located on his main computer in the basement. The defendant said he had been looking at child pornography for four to five years and only looked at children between the ages of eight to

2 At this point, Sgt. Kavanaugh had not read *Miranda* rights to the defendant. However, the conversation remained calm, non-custodial, casual, and not coerced. Defendant was not under arrest at the time.

ten years old. Defendant voluntarily agreed to go to the police station with Sgt. Kavanaugh for a polygraph. At no point did Sgt. Kavanaugh promise the defendant that no charges would be filed if the defendant submitted to a polygraph. At no point did the defendant ask for an attorney.

United States Secret Service Agent Brad Beeler met the defendant in a police interview room and advised him of his *Miranda* rights. The defendant understood these rights and agreed to the polygraph. Exhibits 3 and 4. SA Beeler then initiated a polygraph pre-test interview on the defendant. Defendant told SA Beeler that he first accessed child pornography ten years earlier by utilizing message boards or internet search engines. He began using peer-to-peer networks five years ago. He believed he has download as many as 10,000 files of child pornography including images of children as young as one year old. Most of the children in the child pornography he viewed were around the age of eight to twelve years old. The defendant stated while in Nigeria for business in 1990, he had sex with a girl that he believed to be around thirteen or fourteen years old. The polygraph was administered, the defendant was asked about "hands on" offenses, and the results of the polygraph were inconclusive.

During the post-test questions to the polygraph, the defendant admitted to inappropriate sexual contact with his daughter in 1975 when she was two years old. The defendant admitted to SA Beeler that he rubbed his daughter's "clit" in the bathtub with his finger one time. He also admitted to having inappropriate contact with another two year old who was a friend of his daughters. He digitally penetrated this child, under the clothes, while she was seated on his lap. Further, he mentioned that he touched his three year old grandson's penis to re-direct the boy's penis towards the toilet (the child was urinating and missing the toilet bowl.) While "re-directing" the boy's penis, he thought to himself that his grandson "had a nice or cute penis." The boy is now ten years old so this incident happened about seven years ago. Sgt. Kavanaugh re-interviewed the defendant regarding the statements the defendant made to SA Beeler. This interview was video recorded. The defendant re-stated the aforementioned incidents with children for Sgt. Kavanaugh. At no point during this interview did the defendant ask for an attorney.

iv. Forensics

Det. Steve Grimm of the Regional Computer Crimes Education and Enforcement Group conducted a forensic examination of all of defendant's computers, hard drives, computer-related storage devices, and cell phones. Det. Grimm is a qualified forensic examiner. Det. Partney had submitted 48 pieces of computer equipment seized from the defendant's home for Det. Grimm to analyze. It took Det. Grimm several weeks to complete the analysis due the large volume of evidence and computer devices. Det. Grimm found videos and images of child pornography on twelve of these computer devices. Det. Grimm found some type of evidence of child pornography on fifteen of the forty-eight (48) devices. Det. Grimm also located encrypted files on several of the computer devices. Det. Grimm was unable to open these encrypted files and, thus, does not know what they contain. Det. Grimm also located evidence of peer-to-peer networks, computer-wiping software, search terms related child pornography, and child pornography on the computer devices.

Det. Grimm looked at the defendant's computer, external hard drives, storage devices, thumb drives, and cell phones, which were produced outside of the State of Missouri and traveled in interstate and foreign commerce. Det. Grimm found over 10,000 images of child pornography. The images and videos of child pornography were of prepubescent minor children, both males and females, engaged in sexually explicit conduct, and some portrayed sadistic or masochistic conduct, or other depictions of violence, including bondage. Further, the defendant's Toshiba laptop computer contained the following software applications: CCleaner (used to delete files), TOR browser (which searches the dark web), and Best Crypt (used to encrypt files). Det. Grimm also looked at the defendant's HP Desktop computer. This computer contained TOR software, Shredder software (a program that deletes computer data), 190 animated drawings depicting child sexual abuse, eMule peer-to-peer software, uTorrent application, and images of allocated child pornography. In addition, Det. Grimm discovered search terms related to child pornography and encrypted containers on this computer.

On August 25, 2016, a federal Grand Jury indicted the defendant for one count of Receipt of Child Pornography and two counts of Possession of Child Pornography.

III. LEGAL ANALYSIS OF EVIDENCE SUPPRESSION ISSUES

A. Defendant Does Not Have a Reasonable Expectation of Privacy in Files that He Shared with Third Parties on a Peer-to-Peer Network.

Defendant argues that the undercover downloads of child pornography from his computer by Det. Baine constitute an impermissible warrantless search. As a result, defendant argues that the evidence seized pursuant to the search warrant should be suppressed because the collection of evidence violated his legitimate expectation of privacy on the BitTorrent Network.

The Fourth Amendment protects individuals against "unreasonable searches and seizures" by the government and protects privacy interests where an individual has a reasonable expectation of privacy. *Smith v. Maryland*, 442 U.S. 735, 743-44 (1979). A defendant who is seeking to suppress evidence from a search must demonstrate that he had a "legitimate expectation of privacy" in the place searched. *United States v. Hamilton*, 538 F.3d 162, 167 (2d Cir. 2008). This inquiry involves the court asking two separate questions. First, the court must determine whether the individual had a subjective expectation of privacy. Second, the court must determine whether that expectation of privacy is one that society accepts as reasonable. *Katz v. United States*, 389 U.S. 347, 361 (1967).

[I]n *United States v. Miller*, 425 U.S. 435 (1976), and *Smith*, 442 U.S. 735 (1979), the Supreme Court developed a bright-line application of the reasonable-expectation-of-privacy test that is relevant here. In what has come to be known as the "third-party doctrine," the Court held that "a person has no legitimate expectation of privacy in information he voluntarily turns over to third parties ... even if the information is revealed on the assumption that it will be used only for a limited purpose and the confidence placed in the third party will not be betrayed." *Smith*, 442 U.S. at 743-44 (citing *Miller*, 425 U.S. at 442-44). The Eighth Circuit Court of Appeals in *United States v. Stults*, 575 F3d 834, (8th Cir. 2009) addressed the issue of a person's expectation of privacy on peer-to-peer networks. The Eighth Circuit Court of Appeals followed several other federal courts and found that an individual does not have a reasonable expectation of privacy on a peer-to-peer file sharing network.

The defendant attempts to rely on *Kyllo v. United States*, 533 U.S. 27 (2001); *United States v. Jones*, 565 U.S. 400 (2012); and *Florida v. Jardines*, 133 S.Ct. 1409 (2013). The Supreme Court in *Kyllo* stated,

> [w]e have subsequently applied this principle to hold that a Fourth Amendment search does *not* occur—even when the explicitly protected location of a *house* is concerned—unless "the individual manifested a subjective expectation of privacy in the object of the challenged search," and "society [is] willing to recognize that expectation as reasonable." *Ciraolo, supra,* at 211, 106 S.Ct. 1809. We have applied this test in holding that it is not a search for the police to use a pen register at the phone company to determine what numbers were dialed in a private home, *Smith v. Maryland,* 442 U.S. 735, 743–744, 99 S.Ct. 2577, 61 L.Ed.2d 220 (1979), and we have applied the test on two different occasions in holding that aerial surveillance of private homes and surrounding areas does not constitute a search, *Ciraolo, supra; Florida v. Riley,* 488 U.S. 445, 109 S.Ct. 693, 102 L.Ed.2d 835 (1989). *Id* at 33.

The cases the defendant relied on, *Kyllo, Jones,* and *Jardines,* all involved a search of a person's home or car. In this case, the defendant is on the Internet, a publicly available space, making requests to strangers. The technology used to collect data by law enforcement is not invading his home or his property. It is not even surveilling the defendant's property in anyway. The defendant made his files of child pornography available on a public peer-to-peer file sharing network. The nature of peer-to-peer file sharing is sharing files with complete strangers on the internet. In this case, law enforcement was also on the network and was able to download files from the defendant.

i. No Legitimate Expectation of Privacy when Sharing Files with Unknown Peers on the Network.

Katz vs. United States, 389 U.S. 347 (1967), discusses distinguishing between what an individual has "knowingly exposed to the public" and "what he seeks to preserve as private, even in an area accessible to the public," when determining whether Fourth Amendment protections apply. *Id.* at 353. In this case, BitTorrent is a peer-to-peer file sharing network that facilitates the discovery of computers sharing files.

The defendant is knowingly exposing his communications when sharing and downloading files on BitTorrent with unknown peers. Torrential Downpour did not attempt to gain nor have access to data, other than data the defendant's computer explicitly makes available to other BitTorrent users. After the defendant loads a .torrent file into his/her BitTorrent application, the BitTorrent program will initiate contact with BitTorrent index to locate download candidates. A defendant, through his computer and BitTorrent program, provides the BitTorrent index with certain information, including the defendant computer's IP address and the unique identifier of the .torrent, which contains the instructions on how to download the file(s) that the defendant is seeking to download and/or share. Ex. 2, ¶ 9.

A BitTorrent index does not initiate contact with a defendant or "request" information from a defendant's computer. To the contrary, a defendant, through his computer, voluntarily contacts the BitTorrent index and voluntarily provides the BitTorrent index with the defendant's IP address and the info hash of the data that the defendant is seeking to download or share. In fact, a defendant shares that information with the BitTorrent index for the very purpose of the BitTorrent index, in turn, sharing that information with other potentially unknown peers who possess, or are seeking the same file. Ex. 2, ¶ 10.

The defendant's sharing of information, or "communications" as the defendant defines it, are no longer confined to his home, work, car, or even his own computer. The defendant's communications are shared with the BitTorrent index, which in turn, shares it will other peers who possess or are seeking to possess the same file.

ii. Law Enforcement is not Searching or Seizing Private or Protected Communications; Law Enforcement is a Party to the Communication

In *Smith v. Maryland*, 442 U.S. 735, (1979), the Supreme Court held that telephone numbers dialed from a particular home do not have a "legitimate expectation of privacy" in the numbers dialed, while the contents of the communications do. Here, law enforcement is not intercepting anything. The defendant mischaracterized Torrential Downpour and law enforcement actions in their motion by stating that officers were intercepting data and content. Torrential Downpour does not "intercept" data. The data logged is either (a) data the defendant's computer sent specifically to the law enforcement computer, or (b) data generated by the law enforcement computer. Torrential Downpour did not "hack into" the defendant's computer. The only information available to Torrential Downpour was information that the defendant's computer sent to Torrential Downpour, and in adherence to the BitTorrent file sharing protocol. This is the same data that the defendant's computer would send to any other BitTorrent client.

Torrential Downpour did not attempt to gain nor have access to data routed through the defendant's computer; or to data sent from the defendant's computer, other than data the defendant's computer explicitly sent to the law enforcement computer. BitTorrent is a peer-to-peer file sharing network that facilitates the discovery of computers sharing files, thus the nature of the program requires sharing information with third parties.

The defendant tries to argue that communications in the BitTorrent network are analogous to an email that the defendant sent and law enforcement intercepted. The requests are not analogous to email in the way that the defense contends. In reality, on the BitTorrent network, the defendant’s communication or “email” is being sent to the BitTorrent index and then sent to the law enforcement peer, as opposed law enforcement “intercepting” it. Regardless, BitTorrent is not an anonymous network, and BitTorrent clients announce to the network the torrents that they are sharing as part of their normal operation.

Text messages and email are between specific parties, and the communication are not shared. BitTorrent, on the other hand, announces to the network the torrents that a computer is sharing, unlike a specific email to a specific person. Law enforcement on BitTorrent did not eavesdrop on any communication between the defendant's computer and other parties. Further, the uTorrent software warns users in its’ terms and conditions during the installation that their requests for files and the files stored on their computer are subject to public sharing. So any trust the defendant subjectively put into BitTorrent to protect his privacy interest was misplaced.

Torrential Downpour did not monitor, intercept or record data in transit. The law enforcement computer was the intended recipient of communication, and data was recorded after receipt.

The defendant misplaced his trust when he allowed his system to share files, in this case, with the undercover law enforcement client of BitTorrent. Similar to the situation in *Hoffa vs. United States*, 385 U.S. 293, (1966), the defendant was relying upon his misplaced confidence that his friend would not reveal his wrong doing, when the friend was in fact an undercover government informant. The Supreme Court in *Hoffa*, stated that, "[n]either this Court nor any member of it has ever expressed the view that the Fourth Amendment protects a wrongdoer's misplaced belief that a person to whom he voluntarily confides his wrongdoing will not reveal it." *Id.* at 302. Therefore, the defendant cannot rely on Fourth Amendment protections since on BitTorrent the requests the defendant sent out on the network, as well as, the files he was willing to share, are announced to the other peers on the network, including the law enforcement peer.

In a similar case out of the United States District Court in Vermont, the defendants alleged that law enforcement obtained private information through a warrantless search on a peer-to-peer network. *United States vs Thomas, et. al.* 2013 WL 6000484 (November 8, 2013). The Court found that, "either intentionally or inadvertently, through the use of peer-to-peer file sharing software, Defendants exposed to the public the information they now claim was private." *Id.* at 17. Further, the Court stated that, "because there is no evidence that law enforcement's use of automated software reached information on Defendants' computers that was not made available for sharing by the public, Defendants' motions to suppress on the basis of a warrantless search in violation of the Fourth Amendment must be denied." *Id.* at 20.

Contrary to the defendant's repeated assertions in his motion, Torrential Downpour did not monitor, intercept or record data in transit. The law enforcement computer was the intended recipient of communication, and data was recorded after receipt. Torrential Downpour does not "hack" into a computer. Torrential Downpour is able to download the files from the defendant's computer because the defendant's computer has (a) announced to the network that it is interested in sharing those files, and (b) has made those files available for download to BitTorrent clients.

iii. Current Case Law Regarding Searches on Similar Peer-to-Peer Networks

Courts have rejected the argument that individuals have a reasonable expectation of privacy when using file sharing software. The defendant contends that BitTorrent is different than "old school" peer-to-peer networks, however, that is true only to the technical operation of BitTorrent. It is still a peer-to-peer network, it is still similar to those other peer-to-peer networks in that BitTorrent's purpose is to download files that are "plainly shared."

The Eighth Circuit Court of Appeals in *United States v. Stults,* 575 F3d 834, (8th Cir. 2009) addressed the issue of a person's expectation of privacy on peer-to-peer networks. The Eighth Circuit Court of Appeals followed several other federal courts and found that an individual does not have a reasonable expectation of privacy on a peer-to-peer file sharing network.

> Several federal courts have rejected the argument that an individual has a reasonable expectation of privacy in his or her personal computer when file-sharing software, such as LimeWire, is installed. *See, e.g., United States v. Ganoe,* 538 F.3d 1117, 1127 (9th Cir.2008) (holding that the defendant lacked a reasonable expectation of privacy in the downloaded files stored on his computer, meaning that an agent's use of a file-sharing software program to access child pornography files on the computer did not violate the defendant's Fourth Amendment rights); *United States v. Perrine,* 518 F.3d 1196, 1205 (10th Cir.2008) (holding that defendant had no expectation of privacy in government's acquisition of his subscriber information, including his IP address and name from third-party service providers, where the defendant voluntarily transmitted such information to Internet providers and enabled P2P file sharing on

> his computer, which permitted anyone with Internet access the ability to enter his computer and access certain folders); *United States v. Barrows*, 481 F.3d 1246, 1249 (10th Cir.2007) ("[The defendant] claims that he invited no one to use his computer and therefore expected its contents to remain private. Yet he surely contemplated at least some third-party access: he knowingly networked his machine to the city computer for the express purpose of sharing files."); *United States v. Brese*, No. CR–08–52–D, 2008 WL 1376269 (W.D.Okla. April 9, 2008) (unpublished) ("The Court finds that, notwithstanding any subjective expectation that Defendant may have had in the privacy of his computer, it was not reasonable for him to expect privacy in files that were accessible to anyone else with LimeWire (or compatible) software and an internet connection."); *United States v. Borowy*, 577 F.Supp.2d 1133, 1136 (D.Nev.2008) ("In this case, [the defendant] did not have a legitimate expectation of privacy in files he made available to others using P2P software."). *Id.* at 842-43

In *Stults*, the peer-to-peer network software in question was LimeWire[3]. And while LimeWire works a little differently than BitTorrent, an analogy can be made between the two. Both programs allow users to share files. In both programs, a user is requesting files from unknown users on the same network. On BitTorrent, the network does not operate via shared folders system. Any user that has downloaded a file "indexed" by a torrent automatically shares that file. The Eighth Circuit Court of Appeals in *Stults* found no reasonable expectation of privacy of a user on a peer-to-peer network.

The Sixth Circuit Court of Appeals held in *United States v. Connor*, 2013 WL 1490109, 521 Fed. Appx. 493 (6th Cir. 2013)(unpublished) that a user of a file sharing program does not have a legitimate expectation of privacy. The Court in *Connor* further reasoned that sharing files on peer-to-peer networks is different from sending an email or a letter.

> Conner argues that under *United States v. Warshak*, 631 F.3d 266 (6th Cir.2010) (*en banc*), third-party access to information on one's computer is consistent with a reasonable expectation

---

3 LimeWire is a computer file-sharing program that any user could download for free over the Internet. LimeWire and similar programs connect network participants directly and allow them to download files from one another. To download a file, a LimeWire user opens the application and inputs a search term. LimeWire then displays a list of files that match the search terms and that are available for download from other LimeWire users. When a user downloads a file using the LimeWire network, he or she causes a digital copy of a file on another user's computer to be transferred to his or her own computer. *Stults* at 842.

of privacy in that information. In *Warshak*, we agreed that the government could not compel a commercial ISP to turn over the contents of a subscriber's e-mails without a warrant because subscribers "enjoy a reasonable expectation of privacy in the contents of emails," even though an ISP has the ability to view the contents of e-mail prior to delivery. 631 F.3d at 288. In the context of e-mail, ISPs are "the functional equivalent of a post office or a telephone company," and like an ISP, both of these entities have the ability to intrude on the contents of messages in the course of delivering them to their intended recipients. *Id.* at 286. Since the right or ability of third parties to intrude on phone calls and letters has not been deemed sufficient to defeat a reasonable expectation of privacy in those modes of communication, we agreed that "it would defy common sense to afford emails lesser Fourth Amendment protection" than telephone calls or letters. *Id.* at 285–86.

Warshak does not control this case because peer-to-peer file sharing is different in kind from e-mail, letters, and telephone calls. Unlike these forms of communication, in which third parties have incidental access to the content of messages, computer programs like LimeWire are expressly designed to make files on a computer available for download by the public, including law enforcement. Peer-to-peer software users are not mere intermediaries, but the intended recipients of these files. Public exposure of information in this manner defeats an objectively reasonable expectation of privacy under the Fourth Amendment. *Katz v. United States*, 389 U.S. 347, 351, 88 S.Ct. 507, 19 L.Ed.2d 576 (1967) ("What a person knowingly exposes to the public, even in his own home or office, is not a subject of Fourth Amendment protection."); *see also California v. Greenwood*, 486 U.S. 35, 40–41, 108 S.Ct. 1625, 100 L.Ed.2d 30 (1988) (finding no reasonable expectation of privacy in "plastic garbage bags left on or at the side of a public street," which are accessible by "members of the public" and left on the curb "for the express purpose of conveying [them] to a third party, the trash collector").

Conner responds that he did not know the files he downloaded from LimeWire would be publicly accessible. To prove this point, he emphasizes efforts he made to keep these files private by moving them to compact disks and reinstalling his operating system on the computer to "wipe the hard drive clean." But these efforts only prove that he was ineffective at keeping the files he downloaded from LimeWire from being detected. They do not establish that he was unaware of a risk of being discovered. As the Ninth Circuit observed when confronted with a similar argument, Conner's "subjective intention not to share his files d[oes] not create an objectively reasonable expectation of privacy in the face of [the] widespread public access" to his files LimeWire created. *United States v. Borowy*, 595 F.3d 1045, 1048 (9th Cir.2010) (rejecting Fourth Amendment privacy claim of defendant who unsuccessfully attempted to use LimeWire's privacy features "to prevent others from downloading or viewing the names of files on his computer"). *Connor* at 488 -498.

Also similar to the allegations of the defendant in the case at hand, in *U.S v. Gabel* 2010 WL 3927697 (S.D. Fla. 2010)(unpublished), the defendant alleged that the users on peer-to-peer networks have a reasonable expectation of privacy in their files, thereby protecting them from warrantless searches by law enforcement using enhanced computer programs unavailable to the general public. Magistrate Judge Goodman declined to agreed and found the following, which the District Court adopted,

> The enhanced law enforcement software used in this case did not search any areas of Gabel's computer, download any files, or otherwise reveal any information that was unavailable to ordinary internet users. *Cf. Kyllo v. United States,* 533 U.S. 27, 40, 121 S.Ct. 2038, 150 L.Ed.2d 94 (2001) (holding that when law enforcement “uses a device that is not in general public use, to explore details ... *that would previously have been unknowable* without physical intrusion, the surveillance is a ‘search.’ ”) (emphasis added). Rather, the enhanced software allowed law enforcement to gather and evaluate publically available information with greater efficiency and with an eye towards obtaining probative and admissible evidence of criminal activity.
>
> The Undersigned agrees with every other federal court to have addressed this issue, and finds that users of peer-to-peer networks do not enjoy a reasonable, objective expectation of privacy in the files they share. The Undersigned also agrees with the Ninth Circuit's view in *Borowy* that law enforcement's use of a computer program which allows them to confirm whether the files contain child pornography has no bearing on whether defendants possess a legitimate expectation of privacy in those pornographic files.
>
> Any of the hundreds of thousands (or millions) of users on the Gnutella network could have searched for Gabel's shared files and downloaded those files exclusively from Gabel. That is exactly what law enforcement did here.
>
> The enhanced programs merely permitted law enforcement to more easily organize and classify information that was otherwise available to the public, which aided them in obtaining evidence to support a search warrant. Gabel had no reasonable expectation of privacy in his files. He was, essentially, sharing them with the entire world. *Anyone* with internet access could have easily downloaded Gnutella client software, logged onto the network and downloaded Gabel's files. The fact that law enforcement did so with a device that enabled them to screen for child pornography and collect data for evidentiary purposes does not alter the privacy analysis or in any way shroud Gabel with the Fourth Amendment's protection. It simply means that the police were doing their job. The tool used by law enforcement here is no different, from a constitutional perspective, than the myriad special means—street cameras, radar and canines—that police legally use every day without prior judicial approval to efficiently gather evidence by accessing public information. These police tools do not generate Fourth Amendment concerns because they do not access anything which the public cannot access. Thus, law enforcement's use of an enhanced computer program is the digital equivalent of a pole camera, which is legal and which does not require a warrant or court order. *Id.* 2010 WL 3927697 (September 16, 2010) Report and Recommendations of Defendant’s Motion to Suppress in 10-60168 Sept. 16, 2010 United States District Court for the Southern District of Florida. Adopted by the District Court, Court of Appeals denied to hear argument.

The current case law around the country does not support the defendant's position. Courts have been ruling that: 1) individuals do not have a reasonable expectation of privacy on peer-to-peer file sharing networks; 2) file sharing on peer-to-peer networks is different than sending emails or other protected communication; and 3) law enforcement can use enhanced or modified software to locate individuals sharing child pornography files on peer-to-peer networks.

iv. Plain View Exception

The defendant addresses the "plain view" exception to the warrant requirement in his motion, but this exception does not really fit what Torrential Downpour is doing. Law enforcement is not "intruding" into one's private space and the BitTorrent protocol is matching the law enforcement client with the suspect client to facilitate the download so the file is not really in "plain view."

B. Det. Baine Did Not Search Parts of the Defendant's Computer that was Not Being Shared on the BitTorrent Network. The Evidence Seized was Not Fruit of the Poisonous Tree.

The defendant contends in his motion that the files downloaded by Torrential Downpour from the defendant's computer were from non-public areas of the defendant's computers. The defendant relied on an affidavit from Michele Bush. This argument was fully rebutted by the Government in their response to the defendant's motion to compel. To summarize what the Government argued in their earlier response, Ms. Bush's contention that the files possibly were downloaded by law enforcement from areas of the computer that were not publicly available is completely baseless. First, Ms. Bush did not do an independent forensic examination of the computer devices herself and is relying on a written report from Det. Steve Grimm. Second, Ms. Bush clearly did not fully read Det. Grimm's report as she incorrectly notes that uTorrent was not located on the defendant's computer, when it actually was located on the computer. Third, even though the exact files of child pornography downloaded by Det. Baine were not located by Det. Grimm during his search of the defendant's 48 pieces of computer equipment, that does not mean that the law enforcement software did a warrantless search of non-public areas of the computer to download them. The defendant had plenty of time to store the files in encrypted containers or delete it before the search warrant was executed. It would be **absolutely impossible** to randomly download files from a suspect's computer which are from "unshared folders." Without a torrent file (the instructions), two BitTorrent programs would not be able to share any files. Ex. 2, ¶16. Torrential Downpour cannot search non-public areas of a defendant's computer. It can only locate, after being facilitated through the BitTorrent network, files that other peers on that network have available for download.

There was not illegal search and seizure of evidence with Torrential Downpour, therefore the evidence should not be suppressed.

C. Law Enforcement's Use of Torrential Downpour is Not in Violation of the Electronic Communications and Protection Act nor the Stored Communications Act.

i. Electronic Communications Privacy Act Does Not Apply

The defendant alleged in his motion that law enforcement's use of Torrential Downpour to log IP addresses and torrent info hashes without prior judicial authorization is in violation of the Electronic Communications Privacy Act ("ECPA"). This act is codified under Title 18 U.S.C. § 2510-22. Law enforcement in this case did not violate the ECPA because they did not intercept any contents of the defendant's electronic communications on BitTorrent. The communication came directly to the law enforcement client. Torrential Downpour does not "intercept" data. The data logged is either (a) data the defendant's computer sent specifically to the law enforcement computer, or (b) data generated by the law enforcement computer. Further, even the if the Court finds that defendant's electronic communication collected by law enforcement on BitTorrent was intercepted, the law enforcement node was a party to the communication, thereby excepting them from liability under the ECPA.

The purpose of the ECPA is to control conditions under which the interception of oral and wire communications will be permitted in order to safeguard their privacy. *Lam Lek Chong v. U.S. Drug Enforcement Admin.,* C.A.D.C.1991, 929 F.2d 729, 289 U.S.App.D.C. 136. The ECPA mandates that law enforcement shall receive a proper judicial authorization before intercepting any wire, oral or electronic communication. See 18 U.S.C. §2518. Under the ECPA, "intercept" means the aural or other acquisition of the contents of any wire, electronic, or oral communication through the use of any electronic, mechanical, or other device. 18 USC § 2510(4). The ECPA defines "contents" of electronic communications[4] to include any information concerning the substance, purport, or meaning of that communication. Title 18 U.S.C. § 2510(8).

The information logged by law enforcement is the same information available to all peers on the network, : (1) the IP address of his/her computer, which is necessary to share files between computers on the network (like a delivery address); (2) information exchanged between peers during normal operation, such as the particular BitTorrent client being used; and (3) the content of any files a user is sharing via that peer-to-peer program, which the user – either by

4 The ECPA defines "electronic communication" to mean any transfer of signs, signals, writing, images, sounds, data, or intelligence of any nature transmitted in whole or in part by a wire, radio, electromagnetic, photoelectronic or photooptical system that affects interstate or foreign commerce. Title 18 U.S.C. § 2510(14).

default, or by selection – has made available for other users to download through the peer-to-peer network.

Courts have held that basic user identification information on the Internet is not content of communications. See *In re Zynga Privacy Litigation*, where the Court found that header information, which included a social network user's unique ID and the address of the webpage from which the user's request to view another webpage was sent, did not constitute the contents of any communication under the ECPA, and thus a social networking company and a social gaming company did not violate the ECPA by disclosing referrer header information to third-party advertisers, even if a third-party could use the information to uncover the user's profile page and any personal information made available to the public on that page. *Id.*, C.A.9 (Cal.) 2014, 750 F.3d 1098.

Whether or not, a download on BitTorrent is determined to be "content" information, law enforcement is still a party to the communication. The ECPA statute specifically exempts anyone who is a "party" to the communications. 18 U.S.C. §2511(2)(c). In this case, the law enforcement on BitTorrent is a party to the communication. Since the information is going to the law enforcement client in order to fulfill the download, it is a "party" to the communications and, therefore, excepted from liability under the ECPA.

Similarly, the action of a party to a telephone conversation in recording the conversation with defendant was an "interception" within statutory definition under this chapter, but did not violate the ECPA, which specifically exempts situations in which one party to the conversation is the interceptor. *U.S. v. Turk*, C.A.5 (Fla.) 1976, 526 F.2d 654, rehearing denied 529 F.2d 523, certiorari denied 97 S.Ct. 74, 429 U.S. 823, 50 L.Ed.2d 84. Also see, *Smith v. Cincinnati Post and Times-Star*, which found that there is no "interception" or "eavesdropping" when a party to a conversation, or third person acting with consent of one of parties to the conversation, records that conversation. *Smith v. Cincinnati Post and Times-Star*, C.A.6 (Ohio) 1973, 475 F.2d 740. Therefore, even if the Court were to find that the mere logging of basic information from BitTorrent was an "interception," law enforcement is still not in violation of the ECPA because they were a party to the communication.

In summary, even if the Court were to find that Torrential Downpour had intercepted communication and obtained content, law enforcement was a party to the communication. The information was sent out by defendant's computer to other peers on the network, which included the law enforcement node, and made law enforcement a party to the communication. A party to the communication is excepted from violating the ECPA. It is lawful for a party to a communication to record that communication under ECPA. Torrential Downpour's logging of information as a party to the defendant's electronic communications is lawful.

ii. The Stored Communications Act Was Not Violated By Law Enforcement

The Stored Communications Act (hereafter "SCA"), Title 18 U.S.C. §§2701-2712 regulates how the government can obtain customer records and actual content of communications from telephone companies, email providers, etc. Whenever the government seeks out stored email, it was must comply with the SCA, specifically §2703. In this case, the government did not seek out any stored communications belonging to the defendant. §2702(b)(1) of the SCA permits the disclosure of contents of a communication to the intended recipient. The SCA does not apply because law enforcement did not try and get any information from an electronic service provider ("ESP") or an Internet service provider ("ISP").

D. The Search Warrant Does Not Contain Omissions Pertaining to BitTorrent and Torrential Downpour.

Defendant argues the evidence seized from the residence should be suppressed on the grounds that the search warrant lacked probable cause because it was issued as a result of omissions pertaining to BitTorrent and Det. Baine's use of Torrential Downpour. This argument is belied by the affidavit itself. The search warrant affidavit in this case provided sufficient probable cause.

The Fourth Amendment provides that "no Warrants shall issue, but upon probable cause, supported by Oath or affirmation, and particularly describing the place to be searched, and the persons or things to be seized." U.S. Const. Amend. IV. The issue before the court when reviewing the legal sufficiency of the basis for the issuance of a search warrant is whether the issuing judge had a substantial basis for concluding that probable cause existed. *United States v. White*, 356 F.3d 865, 869 (8th Cir. 2004); *United States v. Terry*, 305 F3d 818, 823 (8th Cir. 2002).

"[P]robable cause does not demand the certainty we associate with formal trials." *Illinois v. Gates*, 462 U.S. 213, 246 (1983). The determination of probable cause is made by a "totality of the circumstances" review. *Id.* at 238. In the context of a search, probable cause is defined as a "fair probability that contraband or evidence of a crime will be found in a particular place." *Id.* The reviewing magistrate is to consider the facts in a practical common sense manner. The evidence must provide the magistrate with a "substantial basis" for his findings. *Id.*,238-9.

In this case, the affidavit provided sufficient probable cause and is not based on omissions of fact. Specifically, the defendant alleges that there was no information in the affidavit about the "computer program used, how it operates, and whether false positives occur." The defendant then makes a completely baseless statement, "false positives are likely to occur when investigating . . ." Doc. #29, ¶ 54. The claim of likely false positives is not correct. The

BitTorrent network makes extensive use of SHA1 hashing to ensure the integrity of the data. See Ex. 2, ¶7. The software has been validated by an independent company. Ex. 2, ¶17, 18. The defendant does not lay out any actual proof or describe which specific facts were intentionally left out to make the affidavit misleading. Nor does the defense explain how by supplementing the "omitted" information, there cannot be a finding of probable cause.

The defendant must offer some evidence beyond mere assertions that an officer made an omission in the affidavit. *United States v. Castillo*, 287 F.3d 21, 26 (1st Cir. 2002).

Omissions are different from misrepresentations and require a different two-step test. The defense "must prove first that facts were omitted with the intent to make, or in reckless disregard of whether they make, the affidavit misleading, and, second, that the affidavit, if supplemented by the omitted information, could not support a finding of probable cause." *United States v. Allen*, 297 F.3d 790, 795 (8th Cir. 2002).

It is well established that "to obtain relief under *Franks*, 'a defendant must first demonstrate that the law enforcement official deliberately or recklessly included a false statement, or omitted a truthful statement from his warrant affidavit." *United States vs Mashek*, 606 F.3d 922, 928 (8th Cir.2010). See also *United States v. McIntryre*, 646 F.3d 1107, 1113-14 (8th Cir.2011)(quoting *Mashek*). Furthermore, before a defendant may receive such a hearing, the reviewing magistrate judge must determine that the allegedly false statement was necessary to the finding of probable cause. *Franks v. Delaware*, 438 U.S. 154 (1978); see also *United States v. Mashek*, 606 F.3d 922, 928 (8th Cir.2010)(citing *United States v. Reinhollz*, 245 F.3d 765, 774 (8th Cir.2001); *United States v. Jansen*, 470F.3d 762, 765-66 (8th Cir. 2006); *United States vs. Sandoval-Rodriguez*, 452 F,3d 984,988 (8th Cir. 2006).

"Allegations of negligence or innocent mistake will not suffice to demonstrate a recklessness or deliberate falsehood." *Mashek*, 660 F.3d at 928 (citing *Franks*, 438 U.S. at 171). "In determining if 'an affiant's statements were made with a reckless disregard for the truth,' the test is whether, after viewing all the evidence, that affiant must have entertained serious doubts as to the truth of his statement or had obvious reasons to doubt the accuracy of the information he reported.'" *McIntyre*, 646 F.3d at 1114 (quoting *United States v. Butler*, 594 F.3d 955, 961 (8th Cir. 2010). "A showing of deliberate or reckless falsehood is not lightly met." *Id.*

The defendant has not met his burden with regard to either prong of *Franks*. A *Franks* hearing should not be granted unless there is actual evidence that the search warrant was invalid. The search warrant is valid on its' face.

In this case, the search affidavit laid out which crime occurred, where it occurred, how it occurred, and how evidence of the crime, including evidence of the perpetrator, would be likely be present at a certain address. Ex. 1. Affidavit. The affidavit specifies that on December 15, 2012, at 11:30 a.m., a computer at the IP address of 76.215.116.247, on the Bit Torrent network was offering to share files of known child pornography. Ex. 1, Affidavit ¶4, 5. The police were able to directly connect with the computer at the IP address, that IP address through the BitTorrent network communicated to the police that it possessed 1128 of 1128 pieces of a known file of child pornography. Ex. 1, Affidavit ¶ 6. The police were able to download from IP address 76.215.116.247 several images of child pornography including the two images described in the affidavit. Ex. 1, Affidavit ¶ 6. Thus, the affidavit has laid out the crimes of receipt and transportation of child pornography occurred on an online network on December 15, 2012 by a person at a certain IP address. The affidavit goes to explain that the ISP reported that the subscriber of the IP address on the date and time of the police download was Roland Hoeffener at 625 Mildred Ave, Webster Groves, Missouri. ¶ 7.

The affidavit goes to explain how peer-to-peer networks, like BitTorrent, operate in paragraphs eleven through nineteen. Ex. 1. Explained in the affidavit is that the software only searches for IP addresses that are possessing or sharing files of known child pornography. Ex. 1, ¶ 5. Paragraphs five, fourteen, and fifteen specifically explain how Det. Baine came across the suspect IP addresses online. Ex. 1. While "Torrential Downpour" is not specifically listed, the brand name of the software is not important to the probable cause determination. Paragraph nineteen explains what information is held within the torrent files on the BitTorrent program. The affidavit does generally explain how the Torrential Downpour software works.

The defendant does not lay out any actual proof or specifically point to which facts were intentionally left out to make the affidavit misleading. Nor does the defense explain how by supplementing the "omitted" information, there cannot be a finding of probable cause. If more information, including very, very specific details how Torrential Downpour operates, was supplemented into the affidavit, that information would only bolster the probable cause. The only operational detail that the affidavit fails to state is that the Torrential Downpour software does a single source download from the defendant's computer, but, again, that detail only bolsters the probable cause, since a single source download means that police are getting the entire download from a solitary download candidate, in this case, the defendant. Search warrant affidavits do not have to contain every detail of the investigation. This affidavit notifies the reviewing Judge in paragraph 2, "since this affidavit is being submitted for the limited purpose of securing a search warrant, your affiant has not included each and every fact concerning this investigation." Ex 1.

The defendant has not met his burden with regard to either prong of *Franks*. A *Franks* hearing should not be granted unless there is actual evidence that the search warrant was invalid.

The search warrant is valid on its' face and there is no evidence that material, intentional omissions occurred.

E. The Judge Authorizing the Warrant was a Neutral Party and Was Capable of Determining Probable Cause.

Warrants may only be signed by an official who is "neutral and detached" and "capable of determining whether probable cause exists for the requested arrest or search." *Shadwick v. City of Tampa*, 407 U.S. 345, 350 (1974). In *Shadwick*, the city authorized municipal clerks, who were supervised by Judges, to issue arrest warrants for ordinance violations. The Supreme Court of the United States affirmed lower court rulings the clerks were qualified to make a probable cause determination to issue the warrants. The Supreme Court in *Shadwick* stated:

"Appellant likewise has failed to demonstrate that these clerks lack capacity to determine probable cause. The clerk's authority extends only to the issuance of arrest warrants for breach of municipal ordinances. We presume from the nature of the clerk's position that he would be able to deduce from the facts on an affidavit before him whether there was probable cause to believe a citizen guilty of impaired driving, breach of peace, drunkenness, trespass, or the multiple other common offenses covered by a municipal code. There has been no showing that this is too difficult a task for a clerk to accomplish. Our legal system has long entrusted nonlawyers *352 to evaluate more complex and significant factual data than that in the case at hand. Grand juries daily determine probable cause prior to rendering indictments, and trial juries assess whether guilt is proved beyond a reasonable doubt. The significance and responsibility of these lay judgments betray any belief that the Tampa clerks could not determine probable cause for arrest." *Shadwick v. City of Tampa*, 407 U.S. 345, 351–52 (1972).

The material set forth in the affidavit relies upon technical computer information, but does not require that either the affiant who prepared the affidavit or the judge who reviews that affidavit have a requisite level of expertise in computer science before rendering a judgement. As the Supreme Court in *Shadwick* noted, our justice system relies on grand juries and trial juries, made up of ordinary citizens, to render judgements in complex and technical cases. If the justice system relies on ordinary citizens to make judgements in complex matters, then an experienced judge, even if lacking expertise in computer science, can also determine whether probable cause exists in a search warrant affidavit for child pornography.

Defendant alleges that due to Judge Richard Bresnahan's, "apparent lack of training in topics related to BitTorrent and complex computer networking he was not able to test the factual basis of the affidavit . . .[i]nstead, his approval served as a rubber stamp for police." Doc. #29, ¶59. A reviewing Judge's role is not to "test" complex computer networks, but instead, to make a practical and common sense decision whether there is a fair probability that contraband or evidence of a crime will be found in a particular place. *Gates*, 462 U.S. at 238. The search warrant affidavit read by Judge Bresnahan described how peer-to-peer file sharing works and how Det. Baine located a person at a specific IP address, offering to share child pornography. A reading of the search warrant affidavit does not necessitate a scientific background. A search warrant in a murder investigation does not require that the affiant have a background in pathology to indicate the cause of death was blunt force trauma nor does the magistrate have to have such a background to review and sign a search warrant in a murder case. Similarly, a search warrant for synthetic drugs not mean that the magistrate judge has to be an expert in organic chemistry.

Defendant goes on to allege in his motions that the Judge's approval, "served as a rubber stamp for police." This a baseless and completely unfounded allegation supported by no facts. The defendant does not present any evidence showing that Judge Bresnahan compromised his ethics and judicial obligation to sign a search warrant in collusion with the police and in violation of the defendant's constitutional rights. The defendant has made no attempt to show that the Judge was not a neutral, unbiased party. The defense cannot simply state that a judge is not neutral, they must point to something in the record that proves this. *United States v. Farlee*, 757 F.3d 810, 820 (8th Cir.), cert. denied, 135 S. Ct. 504, 190 L. Ed. 2d 379 (2014).

An issuing judge's "determination of probable cause should be paid great deference by reviewing courts" and should be upheld if the judge had a "substantial basis for ... conclud[ing] that a search would uncover evidence of wrongdoing." *Gates*, 462 U.S. at 236, 103 S.Ct. 2317 (alteration in original) (internal quotations omitted). There is no reason to believe that Judge Bresnahan was biased or incapable of signing the search warrant.

F. The Images Described by Det. Partney in the Search Warrant Are Child Pornography Under *Dost*. The Defendant has Not Laid a Substantial Basis to Warrant a *Franks* Hearing.

Child Pornography is defined by federal statute as a visual depiction where the production of the visual deception involves the use of a minor engaging in sexually explicit conduct. See 18 U.S.C. Section 2256(8). "[S]exually explicit conduct" is defined to include the "lascivious exhibition of the genitals or pubic area of any person." *Id.* § 2256(2)(A)(v). *United States vs. Dost*, is the leading case on what constitutes "lascivious." 636 F.Supp. 828 (S.D.Cal.1986). In *Dost*, the Court laid our six factors that a trier of fact should look to, among others, to determine if the depiction in question constitutes a lascivious exhibition of the genitals or pubic area. The factors are:

1) whether the focal point of the visual depiction is on the child's genitalia or pubic area;
2) whether the setting of the visual depiction is sexually suggestive, i.e., in a place or pose generally associated with sexual activity;
3) whether the child is depicted in an unnatural pose, or in inappropriate attire, considering the age of the child;
4) whether the child is fully or partially clothed, or nude;
5) whether the visual depiction suggests sexual coyness or a willingness to engage in sexual activity;
6) whether the visual depiction is intended or designed to elicit a sexual response in the viewer.

The Court in *Dost* noted that, "[o]f course, a visual depiction need not involve all of these factors to be a "lascivious exhibition of the genitals or pubic area." The determination will have to be made based on the overall content of the visual depiction, taking into account the age of the minor. *Id* at 832.

In this case, the defense attorney opines that two images of child pornography in the search warrant affidavit may not meet the definition of child pornography. However, both images meet several or all of the factors set forth in *Dost*. The first image titled, "spreadem.chan12\125943702341," is of a young, prepubescent girl approximately eight or nine years old. The child has her legs spread unnaturally with one leg in the air. Her shirt is pulled up exposing her stomach and her skirt is pulled up exposing her underwear. Her underwear has pulled to the side so that half of the child's vagina, specifically the labia majora is exposed in the picture. A darkening of the skin right under the exposed labia majora appears to be the child's anus. The *Dost* factors are clearly met in the photo because: the focal point of the picture is clearly child's genital and pubic area – as her legs are spread very widely to expose it; the setting is sexually suggestive with child's legs open; the child is in an unnatural pose; she is partially dressed, but her underwear is pulled so her labia majora and part of the anus is exposed; the depiction suggests sexual coyness because of how the child is posed; and it is clearly intended to elicit a sexual response in the viewer.

The second picture listed in the search warrant is titled, "spreadem.chan12\125946249912" and depicts a female child approximately eleven to twelve years old laying on her back with her legs in open. The child is wearing a pink sparkly tank top, no pants, and what appears to be "thong" underwear. Her legs are open in a way that her underwear is not completely covering her genitals. The child's pubic hair is clearly exposed and part of one side of the labia majora. The *Dost* factors are clearly met in this photo also: the focal point of the picture is the child's partially clothed genital area – which is front and center in the photograph; as her legs are unnaturally spread very widely to expose the pubic area; the setting is sexually suggestive with child's legs open; she is partially dressed, but her thong underwear is pulled so her pubic hair and part of her labia majora is exposed; the depiction suggests sexual coyness because of how the child is posed; and it is clearly intended to elicit a sexual response in the viewer.

Both photographs listed in the search warrant show a child in a lascivious display of their genitals, therefore, the images meet the definition of child pornography.

Det. Partney's descriptions in the search warrant are accurate representations of the depections. In his summary of the first photograph, he stated the image exposes the side of her vagina and anus –which is true. Half of the child's vagina and a portion of her anus are visible in the picture. As for the second picture, Det. Partney stated that the child's legs are spread with her pubic area exposed and the focal point of the image is her vagina. The child's pubic hairs and part of her labia majora are exposed. The child's genital area is front and center in the photograph. Thus, the photographs constitute child pornography.

In his affidavit, the defense attorney states that each girl is wearing a "bra," however, in each picture the child is wearing a tank-top not a bra. Pictures can be difficult to describe. However, the descriptions by Det. Partney of the images of child pornography were accurate.

At the search warrant application, Det. Partney had the images in his possession to show Judge Bresnahan if the Judge asked to see them. Judge Bresnahan did not ask to look at the images and he signed the search warrant.

Defendant goes on to argue that because he believes the detective's descriptions are overstated, somehow a *Franks* hearing is warranted. The defendant relied on the case of *United States vs. Jacobs*, 986 F.2d 1231 (8th Cir. 1993) and *United States vs. Perkins*, 850 F.3d 1109 (9th Cir. 2017), which are not similar to the case at hand. The *Jacobs* case dealt with an omission in a search warrant affidavit that the drug dog failed to alert to a package. The *Perkins* case dealt with an omission in a federal search warrant that a Canadian constable had reviewed the images and determined that they were not child pornography under Canadian law. In this case, no law enforcement officer that reviewed the images determined they were not child pornography. Neither of these cases is analogous to the case at hand. The pictures depict a lascivious display, with the genital area of children being the clear focal point of both images.

A *Franks* hearing is not warranted. It is well established that "to obtain relief under *Franks*, 'a defendant must first demonstrate that the law enforcement official deliberately or recklessly included a false statement, or omitted a truthful statement from his warrant affidavit." *United States vs Mashek*, 606 F.3d 922, 928 (8th Cir.2010). Omissions are different then misrepresentations and require a different two-step test. The defense "must prove first that facts were omitted with the intent to make, or in reckless disregard of whether they make, the affidavit misleading, and, second, that the affidavit, if supplemented by the omitted information, could not support a finding of probable cause." *United States v. Allen*, 297 F.3d 790, 795 (8th Cir. 2002). Det. Partney did not overstate the descriptions of the photographs and had he shown the images to state court judge, it would have only bolstered the probable cause. The defendant has not made a substantiated preliminary showing to warrant a *Franks* hearing.

IV. LEGAL ANALYSIS OF ARGUMENTS REGARDING DEFENDANT'S STATEMENT

There are two sets of statements at issue in this case. First, there are statements made at the residence shortly after the defendant arrived at his home while the police are executing the search warrant.[5] Second, there are statements made to SA Beeler and Sgt. Kavanaugh at the police department following the search warrant.[6] Defendant argues that the statements made by defendant at his residence should be suppressed because the police did not advise defendant of his Constitutional Rights. Defendant also argues that the statements he provided to the officers were the product of coercion and false promises, and therefore, were not voluntary. Testimony presented at the evidentiary hearing will show that defendant was not in custody when he made statements at his residence. Further, no promises or threats were made to the defendant. The defendant's statements were voluntary. Testimony will also establish that officers properly advised Defendant of his *Miranda* Rights at the police department and defendant voluntarily consented to a polygraph and voluntarily made a statement.

A. Defendant Was Not in Custody When He Made Statements to Law Enforcement Officers at his Residence. Sgt. Kavanaugh Did Not Use Coercion or False Promises to Elicit the Statements From the Defendant.

Sgt. Kavanaugh and members of his unit executed a search warrant on the defendant's home on the evening of April 30, 2013. No one was home when the police arrived. Sgt. Kavanaugh called Mary Beth Hoeffener, the defendant's wife. Sgt. Kavanaugh informed Ms.

---

[5] These statements were audiotaped. A copy of the tape and a transcript of the recording will be made available for the Court to review at the hearing.
[6] These statements were videotaped. A copy of the tape and a transcript of the recording will be made available for the Court to review at the hearing.

Hoeffener of the investigation and asked that her and her husband respond home. About twenty (20) minutes later, Ms. Hoeffener, and her husband responded home. Sgt. Kavanaugh then talked to the defendant, and advised him of the investigation. At this point, law enforcement did not know who was responsible for downloading child pornography. The defendant was not in custody and there was no need to advise him of his *Miranda* rights. There was no restraint of freedom of the degree associated with a formal arrest. At no point did Sgt. Kavanaugh promise the defendant that that no charges would be brought if only evidence of child pornography was found. Hoeffener never asked for an attorney.

Miranda warnings are only required if a suspect is interrogated while in custody. *United States v. Griffin*, 922 F.2d 1343, 1347 (8th Cir. 1990). The ultimate question in determining whether a person is in custody for the purposes of *Miranda* is whether the person is formally arrested or whether his freedom of movement has been restrained to a degree associated with a formal arrest. This Court should first consider the circumstances surrounding the encounter. Second, given those circumstances, this Court should then consider whether a reasonable person would have felt at liberty to terminate the encounter and leave. *See United States v. Perrin*, 659 F.3d 718, 719 (8th Cir. 2011). The Court should not be concerned with how defendant perceived the situation, but rather look to how a reasonable person would view his options in the same circumstances. *Id*. (citing *J.D.B. v. North Carolina*, ___ U.S. ___, 131 S.Ct. 2394, 2402 (2011)). Because the officers had not arrested defendant, the issue is whether there was a restraint of freedom of the degree associated with a formal arrest. *Id*. In making that evaluation, this Court must consider the totality of the circumstances that confronted Defendant at the time of the encounter. *United States v. Czichray*, 378 F.3d 822, 826 (8th Cir. 2004).

In *Griffin*, 922 F.2d at 1349, the Eight Circuit suggested six non-exclusive factors for consideration in making the custody determination: (1) whether the suspect was informed during the interview that the questioning was voluntary, that he could ask the officers to leave, or that he was not considered under arrest; (2) whether the suspect possessed unrestrained freedom of movement during the questioning; (3) whether the suspect voluntarily acquiesced to official questioning or whether the suspect initiated contact with authorities; (4) whether strong arm tactics or deceptive stratagems were employed during questioning; (5) whether the atmosphere of the questioning was police dominated; and (6) whether the suspect was placed under arrests at the termination of the questioning. *Id*.

Following *Griffin*, the Eighth Circuit has emphasized that these factors are simply a rubric for considering the ultimate issue; they are not a mandatory check list. *Perrin*, 659 F.3d at 720. There is no requirement that the *Griffin* analysis be ritualistically followed in every *Miranda* case:

> When the factors are invoked, it is important to recall that they are
>
> not by any means exclusive, and that 'custody' cannot be resolved merely by counting up the number of factors on each side of the balance and rendering a decision accordingly. . . The ultimate inquiry must always be whether the defendant was restrained as though he was under formal arrest. And the court must consider whether the historical facts, as opposed to the one-step-removed *Griffin* factors, establish custody. The debatable marginal presence of certain judicially-created factors that ostensibly tend to 'aggravate the existence of custody' cannot create the functional equivalent of formal arrest where the most important circumstances show its absence.

Czichray, 378 F.3d at 827-28 (emphasis in original).

In *United States v. New*, 491 F.3d 369 (8th Cir. 2007), the Eight Circuit found that statements made to an FBI agent in a hospital room were non-custodial. In *New*, an FBI agent went to a hospital to interview the defendant about a car accident which resulted in two fatalities.

Prior to the agent speaking with the defendant, the defendant had been given a variety of medications due to spinal injuries, difficulty breathing, and pain. The defendant argued that he was physically unable to leave and was in custody during the interview. According to the defendant, as a result of his inability to leave the hospital, the agent should have provided him with *Miranda* warnings prior to questioning him.

The court held that the defendant was not in custody. In its reasoning, the court explained that the agent placed no constraints on the defendant's movement or his ability to communicate with the hospital staff. The agent made "obvious and effective means" of notifying the defendant that he could terminate the interview at any time and would not be arrested.

The application of these principles, then, to the totality of the circumstances facing defendant on April 30, 2013, demonstrates that the defendant was not in custody. When officers arrived at defendant's residence, the defendant was not even home at the time. Officers notified the defendant's wife of the execution of the search warrant at their home via a telephone call and requested them to return home. After the defendant and his wife returned home, Sgt. Kavanaugh made contact with the defendant and advised him of the nature of the police investigation. Sgt. Kavanaugh asked the defendant to accompany him to Sgt. Kavanaugh's vehicle where they could discuss the details of the investigation and the defendant voluntarily agreed. At no point was the defendant handcuffed or restrained, and at the time the defendant was contacted, only Det. Partney and Sgt. Kavanaugh were present in front of the residence. Sgt. Kavanaugh activated a digital recording device to record the conversation as they got into his car. The entire conversation between the defendant and Sgt. Kavanaugh remained calm, non-custodial, casual, and not coerced. Defendant was not under arrest at the time. The atmosphere was not police dominated as questioning was done privately by Sgt. Kavanaugh in the car. Sgt. Kavanaugh did not restrain the defendant or surround him in any way. Further, Sgt. Kavanaugh did not display his weapon. Sgt. Kavanaugh asked the defendant questions and did not compel the defendant to answer in any way. The totality of defendant's circumstances emphatically shows that there was no restraint of freedom of the degree associated with a formal arrest.

Courts have repeatedly refused to find the existence of custody where defendants found themselves in much more police-dominated atmospheres. See, e.g.: *Perrin*, 659 F. 3d at 720-22 (defendant not in custody when questioned in small bedroom by officer wearing side arm after execution of search warrant at defendant's residence by at least six officers in full tactical gear); *United States v. Huether*, 673 F.3d 789, 793-95 (8th Cir. 2012) (defendant not in custody when questioned in bedroom for two hours after execution of search warrant by six officers; officer who conducted questioning was blocking bedroom door); *United States v. Sanchez*, 676 F.3d 627, 629-32 (8th Cir. 2012) (defendant not in custody when questioned by two DEA agents in small, closed door interview room in basement of court house; interviewing agent raised his voice with defendant and called her a liar); *United States v. Boslau*, 632 F.3d 422, 424-29 (8th Cir. 2011) (defendant not in custody when interrogated in small, windowless room at police department for over 40 minutes and questioning shifted from "inquisitorial" to "accusatorial"); *United States v. Muhlenbruch*, 634 F.3d 987, 996-98 (8th Cir. 2011) (defendant not in custody when questioned in small, closed door room at police station); *United States v. Carlson*, 613 F.3d 813, 815-17 (8th Cir. 2010) (statement given to officers at public restaurant not custodial); *United States v. Le Brun*, 363 F. 3d 715, 718-23 (8th Cir. 2004) (defendant not in custody when questioned in windowless room in highway patrol office with enlarged photos on wall as deceptive interview tactic and when officers falsely trumped up evidence they said they possessed); *Czichray*, 378 F.3d at 825-30 (defendant chiropractor not in custody for *Miranda* purposes despite seven-hour interview by two FBI agents in his living room). This abundant precedent demonstrates that the Court should deny Hoeffener's motion to suppress his statements.

After the conversation in the car with the defendant, Sgt. Kavanaugh asked the defendant if he would voluntarily accompany Sgt. Kavanaugh to St. Louis County Police Headquarters and submit to a forensic polygraph. The defendant voluntarily agreed. Sgt. Kavanaugh drove himself and the defendant to police headquarters. At no time during any of the car conversation does the defendant ask for an attorney or attempt to invoke his right to counsel. While en route to the station, the conversation between the defendant and Sgt. Kavanaugh is still being recorded. About half way to the police station, the defendant asks if he will be arrested later and Sgt. Kavanaugh responds, "probably." Sgt. Kavanaugh explained to the defendant that he will most likely be arrested and processed, but not held and will be released that night. At the police station, the defendant asked what Sgt. Kavanaugh was going to tell his wife and the neighbors. Sgt. Kavanaugh told the defendant that he will tell them "nothing" about what is going on. Still at no time does the defendant ask for an attorney. At no time does Sgt. Kavanaugh make any false promises to the defendant.

B. Defendant's Statements at the Police Department were Voluntary

While at the police department, SA Beeler properly advised defendant of his *Miranda* rights using a form and the defendant voluntarily waived those rights and signed the *Miranda* rights form. Exhibit 3. SA Beeler also presented to defendant a consent form for the polygraph test. This form explained that defendant was not being forced to take a polygraph and he was consenting to a polygraph examination out of his own free will. The defendant also signed that form. Exhibit 4. Defendant then voluntarily submitted to a polygraph exam that was not the product of duress or coercion.

The law with respect to *Miranda* waivers is clear. When someone is in custody, law enforcement officers must inform the individual of his or her *Miranda* rights prior to the questioning. *Miranda v. Arizona*, 384 U.S. 436, 444 (1966). The reading of those rights as set forth in *Miranda* are only required when a suspect is in custody and subjected to interrogation. *Id.* At 477-78. After receiving the *Miranda* rights, if a defendant elects to make a statement to law enforcement, the government must show by a preponderance of the evidence that the waiver was knowing, voluntary, and intelligent. *Colorado v. Connelly*, 479 U.S. 157, 169-70 (1986); *North Carolina v. Butler*, 441 U.S. 369, 375-376 (1979). "A waiver is knowing if it is made with a full awareness of both the nature of the right being abandoned and the consequences of the decision to abandon it. It is voluntary if it is the product of a free and deliberate choice rather than intimidation, coercion, or deception." *United States v. Syslo*, 303 F.3d 860, 865 (8th Cir. 2002). (*quoting Moran v. Burbine*, 475 U.S. 412, 421 (1986)). *See also, United States v. Turner*, 157 F.3d 552, 555 (8th Cir. 1998). This determination must be made based upon an examination of the totality of the circumstances surrounding the interrogation. *See Moran*, 475 U.S. at 421. There is no evidence in this case that the defendant had any problem understanding the *Miranda* form. The defendant voluntarily waived his rights and talked to law enforcement.

Sgt. Kavanaugh then re-interviewed the defendant after the polygraph pre-interview and exam by SA Beeler. This interview is videotaped. Sgt. Kavanaugh reminded the defendant that SA Beeler had already reviewed with the defendant his *Miranda* rights and that those rights still applied. Then Sgt. Kavanaugh recapped their earlier encounter at the house. Sgt. Kavanaugh reminded the defendant he was not under arrest at the house. Sgt. Kavanaugh then asked the defendant, “I did not threaten you, right? I did not drag you down here, right?” Defendant nods “yes” to both questions, implying that he did not feel threatened or forced to go to the police station. This interview then re-capped SA Beeler’s earlier interview and polygraph test of the defendant. During this interview, the defendant voluntarily responded to Sgt. Kavanaugh’s questions and even corrected Sgt. Kavanaugh on certain points.

C. Defendant’s Statements Were Not Elicited by Coercion

Defendant argues that his statements should be suppressed because they were elicited by coercion or false promises. As will be demonstrated at the hearing, no threats were made and no force was placed upon the defendant.

Whether a confession is voluntary must be determined by the totality of the circumstances. *Brewer v. Williams*, 430 U.S. 387, 402 (1977). A confession is not voluntary if it is extracted by threats, violence, express or implied promises, such that the defendant's will was overborne and his capacity for self determination was critically impaired. *Sumpter v. Nix*, 863 F.2d 563, 565 (8th Cir. 1988) (citing *Culombe v. Connecticut*, 367 U.S. 568, 602 (1961)). The two factors to consider in applying the “overborne will” doctrine are “the conduct of the law enforcement officials and the capacity of the suspect to resist pressure to confess.” *United States v. Meirovitz*, 918 F.2d 1376, 1379 (8th Cir. 1990), (citing *Colorado v. Connelly*, 479 U.S. 157 (1986)). "Coercive police activity is a necessary predicate to the finding that a confession is not 'voluntary.'” *See Connelly*, at 167.

In *United States v. Brave Heart*, 397 F.3d 1035, 1041 (8th Cir. 2005), the Court noted:

> officers elicit confessions through a variety of tactics, including claiming not to believe a suspect's explanations, making false promises, playing on a suspect's emotions, using his respect for his family against him, deceiving the suspect, conveying sympathy, and even using raised voices. None of these tactics render a confession involuntary, however, unless the overall impact of the interrogation caused the defendant's will to be

overborne. (Internal citations and quotes omitted).

As the testimony and evidence presented at the evidentiary hearing will demonstrate, no threats were made against the defendant and no promises were provided to the defendant. At no time did Sgt. Kavanaugh threaten the defendant. The defendant's will to resist questioning was not overborne. Accordingly, defendant's statement should not be suppressed.

V. **CONCLUSION**

Courts across the country have continually held that an individual does not have reasonable expectation of a privacy on a peer-to-peer file sharing network. Neither the ECPA nor the SCA applies in this case because law enforcement online was a party to the defendant's communication. The defendant's allegations that the reviewing Judge was incapable of reading and signing the warrant are baseless. The defendant's motion to suppress the evidence should be denied.

The defendant was not in custody when he gave statements to Sgt. Kavanaugh at the residence. As a result, Sgt. Kavanaugh did not need to inform him of his *Miranda* rights. Lastly, defendant's statements at the police department were properly obtained from a waiver of *Miranda* and those statements were free from coercion. Based on the foregoing reasons, the Government respectfully requests that the Court deny the defendant's Motions to Suppress Evidence and Statements. The defendant's request for a *Franks* hearing should also be denied as the defendant has not made a substantiated preliminary showing to warrant a *Franks* hearing.

Respectfully submitted,

CARRIE COSTANTIN
Acting United States Attorney

s/ Colleen C. Lang
Colleen C. Lang, #56872MO
Assistant United States Attorney
111 South 10th Street, Room 20.333
St. Louis, MO 63102
(314) 539-2200

CERTIFICATE OF SERVICE

I hereby certify that on May 17, 2017, the foregoing was filed electronically with the Clerk of the Court to be served by email to counsel of record.

s/ Colleen C. Lang
Colleen C. Lang, #56872MO
Assistant United States Attorney